UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/763,673	01/22/2004	Frederic Perriot	20423-08166	7489

34415 7590 11/20/2007

SYMANTEC/ FENWICK
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER
MORAN, RANDAL D

ART UNIT	PAPER NUMBER
2135	

NOTIFICATION DATE	DELIVERY MODE
11/20/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptoc@fenwick.com
bhoffman@fenwick.com
aprice@fenwick.com

Office Action Summary	**Application No.** 10/763,673	**Applicant(s)** PERRIOT, FREDERIC	
	Examiner Randal D. Moran	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 August 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19 and 24-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19,24-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to amendment filed 8/28/2007.

2. Claims 1-19, 24-27 are pending in the application. Claims 20-23 were cancelled in an amendment filed 8/28/2007.

3. Below, Examiner has pointed out particular references contained in the prior art(s) of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claims, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully each reference in its entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Claim Rejections - 35 USC § 101

1. The rejection of **Claims 1-19 and 24-26** under 35 USC 101 is withdrawn in view of amendment filed 8/28/2007.

Claim Rejections - 35 USC § 112

1. The rejection of **Claims 5-13** under 35 USC 112 are withdrawn in view of amendment filed 8/28/2007.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. **Claims 1-13 and 24-26** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Yamamoto (US 5,881,151)**, hereafter "Yamamoto". in view of **Nachenberg (US 5,826,013)**, hereafter "Nachenberg".

3. Considering **Claims 1 and 24,** Yamamoto discloses a method for determining whether computer code contains malicious code (abstract), said method comprising the steps of: optimizing the identified computer code to produce optimized code (column 4- lines 51-55, column 5- lines 26-38, Fig. 3- item 38); subjecting the optimized code to a malicious code detection protocol (column 6- lines 1-4 and 38-50, Fig. 5, Fig. 10) declaring a confirmation that the computer code contains malicious code (column 6- lines 31-37).

Yamamoto does not explicitly disclose identifying computer code suspected of currently containing malicious code, and responsive to the malicious code detection protocol detecting malicious code in the optimized code.

Nachenberg discloses identifying computer code suspected of currently containing malicious code (abstract), and responsive to the malicious code detection protocol detecting malicious code in the optimized code, declaring a confirmation that the computer code contains malicious code (column 12- lines 39-42).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Yamamoto to identify computer code suspected of currently containing malicious code, and responsive to the malicious code detection protocol detecting malicious code in the optimized code, declaring a confirmation that the computer code contains malicious code as taught by Nachenberg to provide a method for detecting polymorphic viruses (Nachenberg- column 1- lines 13-16).

4. Considering **Claims 2 and 25,** the combination of Yamamoto and Nachenberg discloses the malicious code detection protocol is a protocol from the group of protocols consisting of pattern matching, emulation, check summing, heuristics, tracing, X-raying, and algorithmic scanning (Yamamoto- column 7- lines 51-56, column 8- lines 7-20, Fig. 10).

5. Considering **Claims 3 and 26,** the combination of Yamamoto and Nachenberg discloses the optimizing step comprises performing at least one technique from the group of techniques consisting of constant folding, copy propagation, non-obvious dead code elimination, code motion, peephole optimization, abstract interpretation, instruction specialization, and control flow graph reduction (Yamamoto- column 5- lines 32-38)

6.. Considering **Claim 4,** the combination of Yamamoto and Nachenberg discloses at least two of said techniques are combined synergistically (Yamamoto- column 5- lines 26-38).

7. Considering **Claim 5,** the combination of Yamamoto and Nachenberg discloses optimizing code prior to performing virus detection (Yamamoto- Fig. 3).

Yamamoto is silent on the computer code is polymorphic code comprising a decryption loop and a body; and the optimizing step comprises optimizing just the decryption loop.

Nachenberg discloses the computer code is polymorphic code (column 1- lines 14-17) comprising a decryption loop and a body (column 1- lines 25-33); and the optimizing step comprises optimizing just the decryption loop (column 6- lines 54-67, column 7- lines 1-8, Fig. 2- item 200).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Yamamoto to optimize just the decryption loop as taught by Nachenberg in order to substantially reduce the number of file instructions that must be emulated in order to determine whether a target file is infected by a virus (Nachenberg- column 6- lines 56-59).

8. Considering **Claim 6,** Yamamoto discloses optimizing code prior to performing virus detection (Fig. 3).

Yamamoto is silent on optimizing the decryption loop to produce optimized loop code; performing a malicious code detection procedure on the optimized loop code; optimizing the body to produce optimized body code; and subjecting the optimized body code to a malicious code detection protocol.

Nachenberg discloses optimizing the decryption loop to produce optimized loop code (column 6- lines 54-67, column 7- lines 1-8, Fig. 2- item 200); performing a malicious code detection procedure on the optimized loop code (column 6- lines 54-67, column 7- lines 1-8, Fig. 2- item 200); optimizing the body to produce optimized body code (column 6- lines 54-67, column 7- lines 1-8, Fig. 2- item 200); and subjecting the optimized body code to a malicious code detection protocol (column 8- lines 18-37).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Yamamoto to optimize just the decryption loop as taught by Nachenberg in order to substantially reduce the number of file instructions that must be emulated in order to determine whether a target file is infected by a virus (Nachenberg- column 6- lines 56-59).

9. Considering **Claims 7 and 8,** the combination of Yamamoto and Nachenberg discloses the malicious code detection protocol is a protocol from the group of protocols consisting of pattern matching, emulation, check summing, heuristics, tracing, X-raying, and algorithmic scanning (Yamamoto- column 7- lines 51-56, column 8- lines 7-20, Fig. 10).

10. Considering **Claim 9,** the combination of Yamamoto and Nachenberg discloses the step of optimizing the body comprises using at least one output from the group of steps consisting of optimizing the decryption loop and performing a malicious code detection procedure on the optimized loop code (Yamamoto- Fig. 3- item 38, Nachenberg- column 6- lines 63-65, column 7- lines 64-67, column 8- lines 1-4).

11. Considering **Claim 10,** the combination of Yamamoto and Nachenberg discloses when the step of performing a malicious code detection procedure on the optimized loop code indicates the presence of malicious code in the computer code, the steps of optimizing the body and subjecting the optimized body code to a malicious code detection protocol are aborted (Nachenberg- column 11- lines 2-7).

12. Considering **Claims 11 and 12,** the combination of Yamamoto and Nachenberg discloses after the step of performing a malicious code detection procedure on

the optimized loop code, revealing an encrypted body (Nachenberg- column 9- lines 33-38).

13. Considering **Claim 13,** the combination of Yamamoto and Nachenberg discloses the step of revealing an encrypted body comprises applying a key gleaned from the optimized loop code (Nachenberg- column 5- lines 52-58, column 9- lines 33-38).

14. **Claims 14-18 and 20-23** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Yamamoto and Nachenberg** in view of **Chan et al. (US 5,734,908)**, hereafter "Chan".

15. Considering **Claim 14,** the combination of Yamamoto and Nachenberg discloses a method for optimizing computer code that is suspected of containing malicious code (abstract).

the combination of Yamamoto and Nachenberg does not explicitly disclose performing a forward pass operation; performing a backward pass operation; performing a control flow graph reduction; and iterating the above three steps a plurality of times.

Chan does disclose performing a forward pass operation (column 10- lines 34-47 and 56-67, Fig. 5- item 510); performing a backward pass operation (column 6- lines 14-33 and 43-57, Fig. 4A); performing a control flow graph reduction (column 6- lines 1-6); and iterating the above three steps a plurality of times (column 6- lines 14-33, column 7- lines 17-25, Fig. 4A, Fig. 5).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Yamamoto and Nachenberg by performing a forward pass operation; performing a backward pass operation; performing a control flow graph reduction; and iterating the above three steps a plurality of times as taught by Chan in order to more fully utilize the resources of the target machine, thereby enhancing system performance. In particular, the GID unit 116 distributes (moves) instructions from one basic block to other basic blocks (in either the forward or backward direction). The GID unit 116 performs this instruction distribution/movement optimization when it is profitable to do so from an execution viewpoint (that is, when such instruction movement would result in faster executing and tighter resource-utilized object code 118) (Chan- column 3- lines 10-20).

16. Considering **Claim 15,** the combination discloses the iteration of the three steps stops after either: a pre-selected number of iterations; or observing that no

optimizations of the computer code were performed in the most recent iteration (Chan- column 7- lines 36-45, column 11- lines 38-41, Fig. 4A, Fig. 5).

17. Considering **Claim 16,** the combination discloses the step of performing a code motion procedure, wherein the four steps are iterated a plurality of times (Chan- column 6- lines 14-34).

18. Considering **Claim 17,** the combination discloses the forward pass operation comprises at least one of the following steps: peephole optimization; constant folding; copy propagation; forward computations related to abstract interpretation; and instruction specialization (Chan- column 10- lines 34-47, Fig. 5- item 510).

19. Considering **Claim 18,** the combination discloses the backward pass operation comprises at least one of the steps of backward computations related to abstract interpretation and local dead code elimination (Yamamoto- column 5- lines 26-38).

20. **Claim 19** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Yamamoto, Nachenberg** and **Chan** in view of **Lovett et al. (US 2004/0221279),** hereafter "Lovett".

21. Considering **Claim 19,** the combination does not explicitly disclose the backward pass operation comprises the additional step of global dead code elimination.

Lovett does explicitly disclose the backward pass operation comprises the additional step of global dead code elimination ([0091]- line 6, [0104]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Yamamoto and Chan by adding the additional step of global dead code elimination as taught by Lovett in order to transform the IR (intermediate representation) to remove dead regions and thereby reduce the amount of work that must be performed by the target code (Lovett- [0104] lines 8-10).

22. **Claim 27** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Yamamoto** in view of **Lovett.**

23. Considering **Claim 27,** Yamamoto discloses a method for determining whether computer code contains malicious code (abstract), said method comprising the steps of: performing a dead code elimination procedure on the computer code (column 5- lines 26-38, Fig. 3); declaring a suspicion of malicious code in the computer code (column 6- lines 31-37, Fig. 10- S5).

Yamamoto does not explicitly disclose noting the amount of dead code eliminated during the dead code elimination procedure and when the amount of dead code eliminated during the dead code elimination procedure exceeds a pre-selected dead code threshold.

Lovett discloses performing a dead code elimination procedure on the computer code ([0104], Fig. 6- item 75); noting the amount of dead code eliminated during the dead code elimination procedure ([0107]); and when the amount of dead code eliminated during the dead code elimination procedure exceeds a pre-selected dead code threshold ([0133], [0144], [0091] lines 1-2, [0098] lines 9-27).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Yamamoto by noting the amount of dead code eliminated during optimization and declaring a suspicion of malicious code when that amount exceeds a certain threshold in order to prevent the further spread of the virus infection. By outputting the message of the interruption of the process due to the virus infection on the operator console together with the program name or the program number of the object program at the time of interrupting the process, virus infection of a specific program or OS can be notified (Lovett- column 7- lines 43-50).

Response to Arguments

1. Applicant's arguments filed 8/28/2007 have been fully considered but they are not persuasive.

2. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., identifying computer code suspected of currently containing malicious code and declaring a confirmation that the computer code contains malicious code) are not recited in the previously rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). See new combinations and rejections with respect to Claim 1.

3. Regarding **Claim 27,** applicants arguments have been fully considered but are not persuasive. With respect to applicants argument that the combination of Yamamoto and Lovett fails to teach "when the amount of dead code eliminated during the dead code elimination procedure exceeds a preselected dead code threshold." Applicant is directed to Lovett - [0107], [0098], [0091], Yamamoto- column 6- lines 31-37. Lovett discloses group block construction is triggered when the current blocks profiling metrics reaches a trigger threshold. Dead code elimination is a profiling metric. When the dead code list maintained in Lovett reaches a certain threshold (i.e. the trigger threshold), the

combination of Lovett and Yamamoto would generate a warning that the code contains malicious code.

Conclusion

1. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, THIS ACTION IS MADE FINAL. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

2. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Randal D. Moran whose telephone number is 571-270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Thanhnga B. T AU2135

Randal D. Moran
/RDM/

THANHNGA TRUONG
PRIMARY EXAMINER

11/10/2007